Fault Detection, Isolation and Recovery Schemes for Spaceborne Reconfigurable FPGA-Based Systems

This research contributes to a better understanding of how reconfigurable Field Programmable Gate Array (FPGA) devices can safely be used as part of satellite payload data processing systems that are exposed to the harsh radiation environment in space. Despite a growing number of publications about low-level mitigation techniques, only few studies are concerned with high-level Fault Detection, Isolation and Recovery (FDIR) methods, which are applied to FPGAs in a similar way as they are applied to other systems on board spacecraft. This PhD thesis contains several original contributions to knowledge in this field. First, a novel Distributed Failure Detection method is proposed, which applies FDIR techniques to multi-FPGA systems by shifting failure detection mechanisms to a higher intercommunication network level. By doing so, the proposed approach scales better than other approaches with larger and complex systems since data processing hardware blocks, to which FDIR is applied, can easily be distributed over the intercommunication network. Secondly, an innovative Availability Analysis method is proposed that allows a comparison of these FDIR techniques in terms of their reliability performance. Furthermore, it can be used to predict the reliability of a specific hardware block in a particular radiation environment. Finally, the proposed methods were implemented as part of a proof of concept system: On the one hand, this system enabled a fair comparison of different FDIR configurations in terms of power, area and performance overhead. On the other hand, the proposed methods were all successfully validated by conducting an accelerated proton irradiation test campaign, in which parts of this system were exposed to the proton beam while the proof of concept application was actively running.